Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

February 15, 2008 **VIA COURIER**

Hugh Stevenson
Deputy Director, Office of International Affairs
U.S. Federal Trade Commission
600 Pennsylvania Ave. NW, Rm H486
Washington, D.C. 20580 U.S.A.

Dear Mr. Stevenson:

RE: U.S. Federal Trade Commission's possible self-regulatory principles for online behavioral advertising

Thank you for your e-mail of December 21, 2007 asking for my review of the U.S. Federal Trade Commission's (FTC) possible self-regulatory principles for online behavioral advertising ('Proposed Principles'). I have reviewed the Proposed Principles and, as you suggest, materials from the E-havioral Advertising Town Hall the FTC held in November, 2007. I am pleased to provide you with my comments on this important area, and hope you find them helpful as the FTC further develops its principles for online behavioral advertising.

Privacy-enhancing business models really pay off

Privacy can either be treated as a compliance issue or a business issue, but my preference has always been to treat it as a business issue – a business strategy that brings with it a competitive advantage, such as enhanced trust. Overwhelmingly, it seems the members of the Town Hall seem to view privacy as a business issue. This view was well captured in Google Vice President Tim Armstrong's statement: "Google's business model comes down to the word 'trust'." Facebook's Chris Kelly also expressed it well by saying: "What we want is a race to the top around this." I couldn't agree more.

I often speak to businesses and tell them that privacy is a long-term investment, central to retaining existing customers, and essential to attracting new ones. Privacy delivers shareholder value, builds trust, strengthens the value chain, and gives businesses a competitive advantage. This is confirmed by numerous studies, including the research presented to the Town Hall by Lorrie Faith Cranor of Carnegie Mellon University which showed that people will pay more to make their purchase at a privacy-protected website. I captured this notion in my book *The Privacy Payoff: How Successful Businesses Build Customer Trust,* which explains these concepts in detail.

.../2

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
www.ipc.on.ca

The FTC seems to have reviewed several business models in drafting the Proposed Guidelines. For example, the background to the Proposed Guidelines says: "In developing the principles, FTC staff was mindful of the need to maintain vigorous competition in online advertising as well as the importance of accommodating the wide variety of business models that exist in this area." It is also stated in the "Request for Comment" section: "FTC staff recognizes that, to the extent that behavioral advertising supports free web content and other benefits, the choice by consumers not to participate could reduce the availability of such benefits."

Interestingly, a joint study between my office and the Ponemon Institute ("Cross-National Study of Canadian and U.S. Corporate Privacy Practices") found a divergence between our two countries on this point. We found that U.S. corporations tended to view privacy initiatives as restricted to compliance and risk management. In contrast, most Canadian companies believed there was a direct relationship between good privacy practices and enhanced customer trust and loyalty to the brand.

Perhaps the perspective I can offer is that in a privacy-enhanced business model, where it has been shown that privacy can really pay off, the issue of accommodating privacy becomes moot. In the further development of the Guidelines, you may wish to keep in mind that businesses engaged in the models for which the Proposed Principles must be accommodated may be the old guard – businesses that are viewing privacy as a compliance issue rather than a business issue.

The IPC's experience – online behavioral advertising and privacy by design

As you know, "privacy by design" has been my mantra since I published a paper in 1995 with the Netherlands on advancing privacy protection through the pursuit of privacy-enhancing technologies. I was very pleased to hear that this message was repeated by several speakers at your workshop, including Facebook's Chris Kelly and Larry Ponemon. Also, money is increasingly being invested into privacy-enhancing technologies that would allow consumers better ability to exercise choice regarding their personal information, such as Microsoft's roamable opt-out feature and search term scrubbing.

In 1998, I looked at the issue of online behavioral advertising in a paper titled *Data Mining: Staking a Claim on Your Privacy*. In this publication, I reviewed data mining from a fair information practices perspective and discussed the importance of instilling a culture of privacy in organizations. Later that year I examined the issue of online behavioral advertising in a paper titled *Privacy: The Key to Electronic Commerce*. In that paper, I set out that privacy solutions could include: avoiding the collection of personal information in the first place; as well as, the use of privacy-enhancing technologies to either eliminate the use of personal data from transactions, or give direct control for the disclosure of personal information to the individual concerned.

Customer relationship management (CRM) is not new; it is a business strategy which focuses on developing a better understanding of the needs and preferences of customers so that a company can strengthen its relationship with its customer, and marketing is one component of CRM. In 2004, I published with the Canadian Marketing Association a joint report titled "Incorporating Privacy into Marketing and Customer Relationship Management." We outlined in this publication practical steps that businesses can take to integrate fair information practices into their CRM projects.

.../3

As you know, the Internet was not designed to protect identity information. However, I feel that the existing identity infrastructure of the Internet is no longer sustainable, and the level of fraudulent activity online is now threatening to cripple e-commerce. This missing identity layer is a barrier to trust which can prevent customers and citizens from taking advantage of services that are made available to them. In response, last year, my office released *The 7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity In the Digital Age* to make it easier for technology companies to build privacy into their products.

Global Privacy Standard

Online behavioral advertising is a global concern, and as such I would encourage the FTC incorporate the concepts found in the Global Privacy Standard.

Two years ago at the 27th Conference of the International Data Protection Commissioners in Montreux, Switzerland, I chaired a working group of Commissioners convened for the purpose of creating a single harmonized privacy standard. After significant work, we were able to identify the best elements of privacy principles from around the world and harmonize them into a single instrument. This "Global Privacy Standard" builds on the strengths of existing codes containing time honored privacy principles and, for the first time, explicitly recognizes the concept of "data minimization" under the collection limitation principle. The Global Privacy Standard was formally tabled and accepted in the United Kingdom, on November 3, 2006, at the 28th International Data Protection Commissioners Conference.

I am attaching a mapping of the Global Privacy Standard along with comments on how the FTC's Proposed Principles could incorporate aspects of the Global Privacy Standard.

Please do not hesitate to contact me if I can be of any further assistance.

Sincerely yours,

Ann Cavoukian, Ph.D.
Commissioner

Enclosures

Global Privacy Standard	**Comments**
1. Consent: The individual's free and specific consent is required for the collection, use or disclosure of personal information, except where otherwise permitted by law. The greater the sensitivity of the data, the clearer and more specific the quality of the consent required. Consent may be withdrawn at a later date.	Commissioner Jon Liebowitz suggested to the Town Hall "let's start with providing better choices for consumers" instead of "your only choice is take it or leave it." The Honorable Mozelle Thompson pointed out that the public is perfectly willing to exercise choices. To reap the benefits of a privacy-enhanced business model, businesses must realize that a simple yet highly effective customer retention strategy is to assume nothing and always ask. The old business model was "know everything about your customer." The new model is "know everything that your customers want you to know." I noticed that in the FTC's Proposed Principles, consumer control is possible regarding collection of personal information. You may wish to add the ability to consent regarding use, disclosure, and retention of personal information. In addition, you may want to specify in the Proposed Principles that individuals can withdraw consent at a later date. Secondary uses without consent raises concerns, whether it is to combine with offline data, or "anonymous" data. It is especially concerning if it leads to discrimination. If data is truly anonymous, then from my perspective, there is little if any privacy concern. If there is a chance that aggregated data could be later re-identified, then it should be treated as personal information.
2. Accountability: Collection of personal information entails a duty of care for its protection. Responsibility for all privacy related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual within the organization. When transferring personal information to third parties, organizations shall seek equivalent privacy protection through contractual or other means.	You may want to incorporate this principle into the Proposed Principles. As a best practice, it is helpful for organizations to designate an individual actively engaged in design and implementation of online behavioral advertising to ensure that privacy principles are taken into consideration. Also, this principle includes the idea that businesses should put into place policies and practices that give effect to all privacy principles, such as procedures to protect personal information, receive and respond to complaints and inquiries from the public, train staff and communicate information to staff about the business's policies and practices, and to develop information to explain the policies and procedures. This principle works well when there is executive involvement in privacy. That is why I published and recently updated a paper specifically aimed at Boards of Directors called *Privacy and Boards of Directors: What You Don't Know Can Hurt You.*

Global Privacy Standard	**Comments**
3. Purposes: An organization shall specify the purposes for which personal information is collected, used, retained and disclosed, and communicate these purposes to the individual at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.	You may want to include in the Proposed Principles that specifying purposes should be done at or before the time personal information is collected. You may also wish to add that the purpose for the information's use, disclosure and retention should also be specified at the time of collection. You may also want to add that the purposes should be clear, limited and relevant to the circumstances. This could help clarify that companies must not solicit or collect information on an ad hoc basis or engage in "fishing expeditions" to accumulate personal information for an undefined potential future use. Also, this could assist organizations in better articulating how they intend to use personal information (e.g., for marketing purposes, for customer service, to administer a loyalty program, for credit verification, etc.).
4. Collection Limitation: The collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes. Data Minimization – The collection of personal information should be kept to a strict minimum. The design of programs, information technologies, and systems should begin with non-identifiable interactions and transactions as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.	This principle is vitally important and strongly tied to consumer trust which is so critical to a privacy-enhanced business model. I would highly recommend that it be added to the Proposed Principles. Businesses must not collect personal information indiscriminately, in relation to both the amount and the type of information. Data minimization has been recognized by the world's Privacy Commissioners as essential to protecting privacy. For example, Privacy Commissioners from around the world endorsed a resolution on Privacy Protection and Search Engines at the 28th International Data Protection and Privacy Commissioners' Conference in London, United Kingdom in November 2006. The resolution states that "data minimization is key." The more personal information is collected in databases, the more lucrative a target for identity thieves. Identity theft is the fastest growing form of consumer fraud in North America, and the primary cause is an explosive growth in collection of personal information coupled with a steady and easily accessible supply of personal information stored in databases in clear text format (meaning easily read). You may wish to consult our 2005 publication titled *Identity Theft Revisited: Security is Not Enough* for additional information.

Global Privacy Standard	**Comments**
5. Use, Retention, and Disclosure Limitation: Organizations shall limit the use, retention, and disclosure of personal information to the relevant purposes identified to the individual, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.	You may want to add to the Proposed Principles that, not only should retention periods be limited, but also that use and disclosure of personal information should be limited. Also, you may wish to add that use, retention and disclosure should be limited to the relevant purposes identified to the individual. Companies should take special care when destroying or disposing of personal information to ensure that unauthorized parties cannot access or reconstruct the information. You may wish to consult our fact sheet titled *Secure Destruction of Personal Information.*
6. Accuracy: Organizations shall ensure that personal information is as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes.	This is another principle crucial to the success of a privacy-enhanced business model and I would highly recommend that it be added to the Proposed Principles. As advertisers know, customer segments are valuable only to the extent to which they are current. Ensuring that personal information is accurate makes sense from both a business and privacy perspective. If a business has inaccurate or misleading information, this can have an adverse effect on its efforts to identify and market relevant products. Conversely, it may erode a customer's trust in a company. Nicole Wong, Deputy General Counsel at Google, described the potential consequences to the Town Hall: "The greatest harm that we can do is we don't get it right, we serve the wrong ads, we don't target it well, we do it in a way that offends the user, and the whole enterprise fails." Also, according to Don Peppers and Martha Rogers, Ph.D. in their book *Return on Customer*, when a customer is offended by an experience, their equity (the present value of future transactions) goes down AT THAT POINT, even if they complete the transaction they are in. However, once that trust is gained in an online environment, consumers are much more likely to share their personal information. As Don Peppers and Martha Rogers, Ph.D. say in their book *Enterprise One to One: Tools for Competing in the Interactive Age*: "The 1:1 enterprise, operating in an interactive environment, relies not just on information about customers, but information from them." This is where we get into the possibility of permission-based marketing, where consumers are persuaded to volunteer their attention, and which makes consumers active recipients of marketing information, putting control in the hands of consumers. This is a technique which Belgium company Netmining told the Town Hall that it uses.

Global Privacy Standard	**Comments**
7. Security: Organizations must assume responsibility for the security of personal information throughout its lifecycle consistent with the international standards that have been developed by recognized standards development organizations. Personal information shall be protected by reasonable safeguards, appropriate to the sensitivity of the information (including physical, technical and administrative means).	I was pleased to see the portion of the Proposed Principles dealing with security, share similarities with this Global Privacy Standard principle. You may want to add that security should be ensured throughout the lifecycle of the information. Also, you may wish to add for greater clarity that the safeguards should include physical, technical and administrative means. Hackers are no longer the main cause of identity theft. It is usually accomplished through an inside job, such as a rogue employee. Poor information management practices are largely at fault in these cases. Also, personal information should be encrypted when it is stored in a database or transmitted over the Internet. Businesses should watch out for information walking out the door on mobile devices such as laptops and PDAs. You may wish to consult our publication titled *Safeguarding Privacy in a Mobile Workplace.*
8. Openness: Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals.	The Proposed Principles include a transparency principle. The Global Privacy Standard principle on openness refers to transparency in a somewhat different context, which is essentially related to the accountability principle – making policies and practices readily available to individuals above and beyond specifying purposes. Individuals are increasingly aware and conscious of their privacy rights, and customers should be able to easily acquire information about a company's privacy policies and procedures.
9. Access: Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.	Martha Rogers, Ph.D., in her book *Return on Customer* explains the value of getting information from customers directly: "Personal information has great value: the closer it is to the customer, value is reduced as information moves away from the individual, value is enhanced with the use of consent, increasing the value of the personal information you hold increases your brand value for privacy." Advertisers know that accuracy of information and honest dealings are critical components of successful customer relationships. When asked, companies must share the personal information they hold about individual customers and amend any inaccurate data. They should also provide specifics about any third parties to which they have disclosed personal information, to the best of their ability. If a customer successfully demonstrates that the personal information is inaccurate or outdated, the organization must correct the information as quickly as possible.

Global Privacy Standard	**Comments**
10. Compliance: Organizations must establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal. Organizations shall take the necessary steps to monitor, evaluate, and verify compliance with their privacy policies and procedures.	You may wish to add to the Proposed Guidelines this concept that organizations must develop a system to respond to complaints.

Creation of a Global Privacy Standard

By Commissioner Ann Cavoukian, Ph.D.

Introduction

In 2005, at the 27th International Data Protection Commissioners Conference in Montreux, Switzerland, I chaired a Working Group of Commissioners. This Working Group was convened for the sole purpose of creating a single Global Privacy Standard. Faced with globalization and convergence of business practices, regardless of borders, I thought there was a pressing need to harmonize various sets of fair information practices into one Global Privacy Standard. Once such a foundational policy piece was in place, then businesses and technology companies could turn to a single instrument for evaluating whether their practices or systems were actually privacy enhancing, in nature and substance.

While attempting to develop a single law on data protection was beyond our reach, I was confident that we could develop a single privacy instrument, globally. In advancing my objective to develop a harmonized set of fair information practices, my office embarked on the preliminary work of conducting a "Gap Analysis." This was the process of comparing leading privacy practices and codes from around the world, comparing their various attributes, and the scope of the privacy principles enumerated therein. We identified the strengths and weaknesses of the major codes in existence and then tabled our Gap Analysis with the Working Group of Commissioners.

In the months that ensued, we embarked upon the work of harmonizing the principles into a single set of fair information practices. This led to the development of the attached Global Privacy Standard (GPS), which builds upon the strengths of existing codes containing time-honoured privacy principles and, for the first time, reflects a noteworthy enhancement by explicitly recognizing the concept of "data minimization" under the "collection limitation" principle.

After successive drafts of the GPS were developed, revised and circulated for review, the attached final version of the GPS was formally tabled and accepted in the United Kingdom, on November 3, 2006, at the 28th International Data Protection Commissioners Conference.

Objective

The objective of the Global Privacy Standard is to form a set of universal privacy principles, harmonizing those found in various sets of fair information practices presently in existence.

The Global Privacy Standard draws upon the collective knowledge and practical wisdom of the international data protection community.

Scope

The Global Privacy Standard reinforces the mandate of privacy and data protection authorities by:

- focusing attention on fundamental and universal privacy concepts;
- widening current privacy awareness and understanding;
- stimulating public discussion of the effects of new information and communication technologies, systems, standards, social norms, and laws, on privacy; and
- encouraging ways to mitigate threats to privacy.

The GPS informs developers and users of new technologies and systems that manage or process information. The GPS may be particularly useful when developing information and communication technology standards, specifications, protocols, and associated conformity assessment practices.

The GPS can assist public policymakers when considering laws, regulations, programs and the use of technologies that may impact privacy. The GPS can equally assist businesses and developers of technology that may have an impact on privacy and personal information.

The GPS addresses privacy concerns for decision-makers in any organization that has an impact on the way in which personal information is collected, used, retained, and disclosed.

The GPS is not intended to pre-empt or contradict any other laws or legal requirements bearing upon privacy and personal information in various jurisdictions.

GPS Privacy Principles

1. **Consent:** The individual's free and specific consent is required for the collection, use or disclosure of personal information, except where otherwise permitted by law. The greater the sensitivity of the data, the clearer and more specific the quality of the consent required. Consent may be withdrawn at a later date.

2. **Accountability:** Collection of personal information entails a duty of care for its protection. Responsibility for all privacy related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual within the organization. When transferring personal information to third parties, organizations shall seek equivalent privacy protection through contractual or other means.

3. **Purposes:** An organization shall specify the purposes for which personal information is collected, used, retained and disclosed, and communicate these purposes to the individual at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.

4. **Collection Limitation:** The collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.

> **Data Minimization** -- The collection of personal information should be kept to a strict minimum. The design of programs, information technologies, and systems should begin with non-identifiable interactions and transactions as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.

5. **Use, Retention, and Disclosure Limitation:** Organizations shall limit the use, retention, and disclosure of personal information to the relevant purposes identified to the individual, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.

6. **Accuracy:** Organizations shall ensure that personal information is as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes.

7. **Security:** Organizations must assume responsibility for the security of personal information throughout its lifecycle consistent with the international standards that have been developed by recognized standards development organizations. Personal information shall be protected by reasonable safeguards, appropriate to the sensitivity of the information (including physical, technical and administrative means).

8. **Openness:** Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals.

9. **Access:** Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. **Compliance:** Organizations must establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal. Organizations shall take the necessary steps to monitor, evaluate, and verify compliance with their privacy policies and procedures.

Published: November 8, 2006